EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview and email with Eric Shelton on 4/22/10.

The application has been amended as follows:

List of Amended Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for enabling identification of at least one address associated with ingress of a packet stream, comprising:

identifying a portion of a packet data communication network as a trusted region;

identifying all border devices at entry points on an outer boundary of the trusted region of the network;

configuring each respective one of the border devices to mark predetermined packets transmitted into the trusted region of the network, each marking of a packet by a respective border device comprising providing a fragment of a network address of the respective border device with the packet;

receiving a plurality of marked packets from one of the border devices; and

processing address fragments from the received marked packets to reconstruct the network address of the one border device,

wherein each respective one of the configured border devices performs the following steps:

fragmenting the address of the respective border device into a first plurality of overlapping fragments of a first format;

assigning fragment identifiers of a first range to the first plurality of fragments; and

marking a first plurality of packets forwarded into the trusted region by including one of the first plurality of overlapping fragments and including a corresponding assigned fragment identifier of the first range in each of the first plurality of packets forwarded by the respective border device.

2. (Original) The method of claim 1, wherein the configuring step comprises causing each respective border device to mark all packets being transmitted into the trusted region of the network.

3. (Original) The method of claim 1, wherein the configuring step comprises causing each respective border device to mark all packets being transmitted to a predetermined destination through a region of the network trusted by the predetermined destination.

4. (Original) The method of claim 1, wherein the identified border devices comprise a plurality of routers of one or more autonomous systems of the packet data communication network.

5. (Original) The method of claim 4, wherein the packet data communication network is the Internet.

6. (Original) The method of claim 4, wherein the plurality of routers include routers on a backbone of one or more autonomous systems.

7. (Currently Amended) The method of claim 1, wherein each respective one of the configured border devices further performs the following steps:

fragmenting the address of the respective border device into a second plurality of overlapping fragments of a second format;

assigning fragment identifiers of a second range to the second plurality of fragments; and

marking a second plurality of packets forwarded into the trusted region by including one of the second plurality of overlapping fragments and including a corresponding assigned fragment identifier of the second range in each of the second plurality of packets forwarded by the respective border device.

8. (Currently Amended) The method of claim 7, wherein:

the first plurality of fragments are formatted to comprise sequential sections of the address of the respective border device having a predetermined number of bits of overlap between consecutive ones of the sequential sections; and

the second plurality of fragments are formatted so that each of the second plurality of fragments comprises two offset sections of the address of the respective border device, at least one pair of fragments included in the second plurality of fragments having a predetermined number of bits of overlap.

9. (Currently Amended) The method of claim 7, wherein the step of processing address fragments from the received marked packets to reconstruct the network address of the one border device comprises:

processing fragments from said plurality of marked packets received from the border device having identifiers in the first range to compare overlapped bits and combine fragments having matching overlapping bits to a form a first copy of the address of the one border device from the first fragments;

processing fragments from said plurality of marked packets received from the border device having identifiers in the second range to compare overlapped bits and combine fragments having matching overlapping bits to form a second copy of the address of the one border device from the first fragments; and

recognizing a valid reconstructed address if the first and second copies of the address of the one border device match.

10. (Original) The method of claim 1, wherein the predetermined packets include packets of a type selected from the group consisting essentially of: packets relating to a denial of service attack; packets containing spam e-mail messages; high volume traffic and packets containing illegally distributed content.

11. (Currently Amended) The method of claim 1, in combination with at least one step for imposing control on a flow of packets through the one border device whose network address was reconstructed from fragments in received marked packets.

12. (Currently Amended) The method of claim 11, wherein the at least one step of imposing control comprises causing the one border device to block transmission into the trusted region of the network of packets addressed to a predetermined destination.

13. (Currently Amended) The method of claim 1, wherein the packet data communication network transports Internet Protocol (IP) type packets comprising headers and data, and each marking of a packet comprises inserting the fragment of the network address of the respective border device into a predetermined field of the IP header of the marked packet.

14. (Original) The method of claim 13, wherein the predetermined field comprises a Fragmentation Offset field of the IP header.

15. (Original) The method of claim 13, wherein the predetermined field comprises a Identification field of the IP header.

16. (Original) The method of claim 13, wherein the predetermined field comprises a Fragmentation Offset field and the Identification field of the IP header.

17. (Currently Amended) The method of claim 16, wherein the fragments are portions of IP addresses.

18. (Currently Amended) A method of marking communication packets forwarded by a border device through a packet data communication network with router identifying information, comprising:

identifying a portion of a packet data communication network as a trusted region;

marking predetermined packets transmitted into the trusted region of the network by performing the steps of:

fragmenting a network address of the ~~router~~ border device into a first plurality of overlapping address fragments of a first format;

assigning fragment identifiers of a first range to the first fragments; and

including one of the first plurality of fragments and including a corresponding assigned fragment identifier of the first range in each of a first plurality of packets forwarded by the ~~router~~ border device.

19. (Currently Amended) The method of claim 42, wherein:

the first plurality of address fragments are formatted to comprise sequential sections of the network address of the border device having a predetermined number of bits of overlap between consecutive ones of the sequential sections; and

the second plurality of address fragments are formatted so that each second address fragment comprises two offset sections of the address of the border device, at least one pair of fragments included in the second plurality of address fragments having a predetermined number of bits of overlap.

20. (Currently Amended) The method of claim 42, further comprising forming a hash value from each respective fragment, wherein when each respective fragment is included in a particular packet the hash value formed from the respective fragment is also included in the particular packet.

21. (Currently Amended) A method of reconstructing a network address of a packet marking device comprising:

receiving a first plurality of data packets containing marks comprising fragments of [[a]] the network address of the packet marking device and respective fragment identifiers in a first range, via [[the]] a packet data communication network;

for each respective fragment from the first plurality of data packets, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from a first plurality of previously received packets, to determine if there is a match between the respective fragment and a fragment from one of the first plurality of previously received packets; and

for each match between a respective fragment from the first plurality of data packets and a fragment from [[a]] the first plurality of previously received ~~packet~~ packets,

concatenating one of the matching fragments with non-matched bits of the other one of the matching fragments,

wherein the matching and concatenation is performed until a combination of fragments produces the network address of the packet marking device that marked the first plurality of data packets.

22. (Currently Amended) The method of claim 21, wherein the network address is an Internet Protocol (IP) address of a router on a border of a trusted region of the packet data communication network.

23. (Original) The method of claim 22, wherein the packet data communication network is the Internet.

24. (Currently Amended) The method of claim 23, wherein the network address identifies an ingress point of the flow of packets representing an attack on at least one target served through the trusted region.

25. (Currently Amended) The method of claim 23, wherein the network address identifies an ingress point of a flow of packets containing spam e-mails.

26. (Currently Amended) The method of claim 23, wherein the network address identifies an ingress point of a flow of packets containing illegal information content.

27. (Currently Amended) The method of claim 21, wherein:

the matching and concatenation for the first plurality of data packets is performed on fragments assigned identifiers in the first range and produces a first version of the network address;

the method further comprises:

receiving a second plurality of data packets containing marks comprising fragments of the network address of the packet marking device and respective fragment identifiers in a second range, via the packet data communication network;

for each respective fragment from the second plurality of data packets containing a fragment identifier in the second range, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from a second plurality of previously received packets carrying identifiers in the second range, to determine if there is a match between the respective fragment and a fragment from one of the second plurality of previously received packets; and

for each match between a respective fragment from the second plurality of data packets containing a fragment identifier in the second range and a fragment from the second plurality of previously received packets containing a fragment identifier in the second range, concatenating one of the matching fragments with non-matched bits the other one of the matching fragments,

wherein the matching and concatenation for fragments from packets containing fragment identifiers in the second range is performed until a combination of fragments

produces a second version of the network address of the packet marking device that marked the second plurality of data packets.

28. (Currently Amended) The method of claim 27, further comprising validating the network address if the first version and the second version match.

29. (Currently Amended) The method of claim 21, further comprising:

for each received data packet containing a mark, recovering and storing a hash value related to a respective mark from the received data packet containing the respective mark;

upon deriving the network address, examining stored hash values corresponding to fragments used to derive the network address; and

identifying the network address as relating to a source of an attack if at least a predetermined number of hash values corresponding to fragments used to derive the network address have been received and stored.

30. (Currently Amended) The method of claim 29, wherein the step of examining comprises:

forming a hash of the network address;

fragmenting the hash of the network address; and

comparing the hash fragments to the stored hash values corresponding to fragments used to derive the network address.

31. (Currently Amended) A border device for communication through a packet data communication network, comprising:

a communication interface for enabling transmission of packets through the packet data communication network; wherein

the border device is programmed to receive packets from outside of a trusted region of the packet data communication network, mark predetermined ones of the received packets, and forward the marked packets into the trusted region by performing steps comprising:

a) fragmenting a network address of the border device into a first plurality of overlapping fragments of a first format;

b) assigning fragment identifiers of a first range to the first fragments;

c) including one of the first plurality of fragments and including a corresponding assigned fragment identifier of the first range in each of a first plurality of packets forwarded by the border device into the trusted region.

32. (Currently Amended) The border device as in claim 31, wherein the border device is a router comprising an input port processor in a line card of the router.

33. (Currently Amended) The border device as in claim 31, wherein the border device is a router comprising a content addressable memory for use in determining if individual packets should be marked.

34. (Currently Amended) A computer system programmed to implement a sequence of steps, to identify a packet marking device at or near a point of origin of a particular flow of packets through a packet data communication network, the sequence of steps comprising:

receiving data packets each containing a mark comprising a fragment of a network address of the device, via the packet data communication network;

for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets to determine if there is a match between the respective fragment and a fragment from a previously received packet; and

for each match between a respective fragment from a newly received packet and a fragment from a previously received packet, concatenating one of the matching fragments with non-matched bits of the other one of the matching fragments,

wherein the matching and concatenation is performed until a combination of fragments produces the network address of [[a]] the packet marking device.

35. (Currently Amended) A computer program product comprising executable code embodied in a non-transitory machine-readable medium, execution of the code causing a computer to perform a sequence of steps to identify a device at or near a point of

origin of a particular flow of packets through the network, the sequence of steps comprising:

receiving data packets containing marks comprising fragments of a network address, via the packet data communication network;

for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets to determine if there is a match; and

for each match between a respective fragment from a newly received packet and a fragment from a previously received packet, concatenating one of the matching fragments with non-matched bits of the other one of the matching fragments,

wherein the matching and concatenation is performed one or more times until a combination of fragments produces a complete address of a device that marked a plurality of the received packets.

36 – 41. (Canceled)

42. (New) The method of claim 18, further comprising:

fragmenting the network address of the border device into a second plurality of overlapping address fragments of a second format;

assigning fragment identifiers of a second range to the second fragments; and

including one of the second plurality of fragments and including a corresponding assigned fragment identifier of the second range in each of a second plurality of packets forwarded by the border device.

43. (New) The border device of claim 31, wherein the border device is further programmed to perform the steps of:

d) fragmenting the network address of the border device into a second plurality of overlapping fragments of a second format;

e) assigning fragment identifiers of a second range to the second fragments;

f) including one of the second plurality of fragments and including a corresponding assigned fragment identifier of the second range in each of a second plurality of packets forwarded by the border device.

REASONS FOR ALLOWANCE

1. The following is the examiner's statement of reasons for allowance:

Independent claims 1, 18, 21, 31, and 34 among other things teach:

The limitations found in independent claim 1, 18, 21, and 34 with the additional limitations of claim 7. The limitations are identifying a trusted region, by identifying incoming packets at border devices. The border devices are configured to mark incoming packets into the trusted region. The marking of packets includes a fragment of a network address of the border device. The ability to process the address fragments to be able to reassemble the network address of a given border device. A configured border device is able to fragment the address of the respective border device into a plurality of overlapping fragments of a first format. The Range of fragments are assigned fragment identifiers. The trusted region has the plurality of packets which was marked.

2. The closes prior art of record are Munger(2002/0161925), Poetto(2003/0145232). See remarks dated 11/19/2009 for differences in these applications compared to current invention.

3. For these reasons, in conjunction with all other limitations in this particular claim, puts this case in condition for allowance.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

CORRESPONDANCE INFORMATION

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GERALD SMARTH whose telephone number is (571)270-1923. The examiner can normally be reached on Monday-Friday(7:30am-5:00pm)est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu can be reached on (571)272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/GERALD SMARTH/

Examiner, Art Unit 2446

/Benjamin R Bruckart/

Primary Examiner, Art Unit 2446